HOUGH BREMNER INC.
(REGISTRATION NO. 2020/672478/21)

POLICY:
Protection of Personal Information Act No.04 of 2013

HOUGH BREMNER INC.
admin@houghbremner.co.za

Contents

1. CONTACT PARTICULARS

Head of business:	Mr DC Eastes
	Mrs. C Lundy
Postal Address:	P.O. Box 642
	Mbombela
	Mpumalanga
	1200
Telephone Number:	013 752 3177
Fax Number:	013 752 3514
E-mail Address:	admin@houghbremner.co.za
Website:	www.houghbremner.co.za
Information Officers:	Mrs. I Aucamp
	Mr P Vuma
Physical Address:	30 Van Rensburg Street
	Mbombela
	Mpumalanga
	1200

2. DEFINITIONS

"**biometrics"** means a technique of personal identification that is based on physical, physiological or behavioral characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

"**child"** means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;

"**competent person"** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child; "consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

"**Constitution"** means the Constitution of the Republic of South Africa, 1996;

"**data subject**" means the person to whom personal information relates;

"de-identify", in relation to personal information of a data subject, means to delete any information that—

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, and

"**de-identified**" has a corresponding meaning;

"**direct marketing**" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of—

(a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

(b) requesting the data subject to make a donation of any kind for any reason;

"electronic communication" means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"**enforcement notice"** means a notice issued in terms of section 95;

"**filing system**" means any structured set of personal information, whether centralized, decentralized or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

"FICA" means Financial Intelligence Centre Act No. 38 of 2001; *RMCP Policies for Hough Bremner Inc are available on request and on our website.*

"information matching program" means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject;

"**Information Officer"** of, or in relation to, a—

(a) **public body** means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or

(b) **private body** means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

"Minister" means the Cabinet member responsible for the administration of justice;

"**Operator**" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

"**Parties**" means the client/s and/or employee/s of the responsible party;

"Person" means a natural person or a juristic person;

"**Personal Information**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

“prescribed” means prescribed by regulation or by a code of conduct; “private body” means—

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or profession; or

(c) any former or existing juristic person, but excludes a public body;

“processing” means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

(a) the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

“professional legal adviser” means any legally qualified person, whether in private practice or not, who lawfully provides a client, at his or her or its request, with independent, confidential legal advice;

“Promotion of Access to Information Act” means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

“**public body**” means—

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

(b) any other functionary or institution when—

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation;

“**public record**” means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

“records” means any recorded information—

(a) regardless of form or medium, including any of the following—

(i) Writing on any material;

(ii) information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing;

(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

(b) in the possession or under the control of a responsible party;

(c) whether or not it was created by a responsible party; and

(d) regardless of when it came into existence;

"**Regulator"** means the Information Regulator established in terms of section 39;

"re-identify", in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that—

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, and "re-identified" has a corresponding meaning;

"**Republic"** means the Republic of South Africa;

"**Responsible Party**" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

"restriction" means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

"**special personal information**" means personal information as referred to in section 26;

"this Act" includes any regulation or code of conduct made under this Act; and

"**unique identifier**" means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

3. INTRODUCTION

Hough Bremner Inc. (Registration Number 2020/672478/21) is a legal practice that is duly registered with the Legal Practice Council of the Republic (F66963) and Financial Intelligence Centre (AI/110304/00074). In terms of Protection of Person Information Act No.04 of 2013 (hereinafter, the Act), Hough Bremner Inc. is a Responsible Party.

4. PURPOSE OF THE POLICY

The purpose of the policy is to comply with the provisions of the Act, and to promote ethical and professional conduct. The primary purpose of the policy and the Act is to:

(a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—

(i) balancing the right to privacy against other rights, particularly the right of access to information; and

(ii) protecting important interests, including the free flow of information within the Republic and across international borders;

(b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

(c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and

(d) establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

5. ACCESS TO DOCUMENTS

Personal Information of the Parties that is in the custody of the Responsible Party must be kept confidential, however, such information may be disclosed in the following circumstances:

5.1 Where consent to disclose has been granted by the Parties.

5.2 Where the Responsible Party is required to disclose by law or court order, *inter alia*, to comply with tax reporting and FICA requirements.

5.3 Where it is necessary to protect the legitimate interest of the Responsible Party. For example, if the Parties owe the Responsible Party money/fees for services rendered. The

Responsible Party may disclose the Parties' Personal Information in pursuance of recovering the amount due to it.

6. SECURITY & DISCLOSURE

6.1 The Responsible Party is committed to ensuring that Personal Information is secured; and internal controls to prevent unauthorized access and disclosure are applied and tested by internal (quarterly) and external (Annually) auditors. PAIA Manual can be requested.

6.2 Personal Information may be given to another person or external party after the Parties have submitted a request to the Responsible Party. The Responsible Party may not unreasonably reject or refuse the request. The request must be made in writing and submitted to the Information Officer in terms of Promotion of Access to Information Act No.02 of 2000. The request must be supported by reasons, and a fee may be charged by the Responsible Party for processing the request.

7. STORAGE / RETENTION OF DOCUMENTS

7.1 The records and documents are stored in lockable facilities of the Responsible Party, and movement of such is subjected to strict procedures. The contravention of the internal procedures by the staff of the Responsible Party will trigger disciplinary procedures against the perpetrator/s.

7.2 In terms of section 56(2) of Unemployment Insurance Act No.63 of 2001, the Responsible Party must retain Personal Information of its staff. Furthermore, section 29 and 30 of Tax Administration Act No. 28 of 2011 also provide that Person Information must be retained for Seven years; and in cases where the Commissioner of South African Revenue Services (hereinafter, SARS) has already invoked an audit over a particular transaction, all records affecting the transaction must be retained until the audit is concluded even if the audit's period is longer than Seven years.

7.3 Paragraph 14(1) of Schedule 4 of the Income Tax Act No. 58 of 1962, provides that Responsible Party must retain party of Personal Information of every employee for a period of five years from the date of submission of tax returns to SARS. The Responsible shall retain records showing the amounts of remuneration paid or due by him to such employee and the amount of employees' tax deducted or withheld from each such amount of remuneration, and such record shall be retained by the employer and shall be available for scrutiny by SARS.

7.4 In addition to the above legislative requirements, the Responsible Party shall retain the records in order to comply with statutory obligations which may be applicable and relevant, henceforth.

8. DESTRUCTION OF DOCUMENTS

8.1 Personal Information collected by the Responsible Party will be destroyed upon fulfillment of the purpose it was collected for, and compliance with the relevant legislation.

8.2 The Responsible Party shall take all reasonable steps to ensure that before the records or/and files are destroyed, there are no original documents, therein. If original documents are found, they must be returned to the provider of such records.

8.3 Destruction and removal of records shall be authorized by the director/s of the Responsible Party.

9. TERMINATION OF THE MANDATE / CONTRACT

9.1 In relevant matters, upon termination of the mandate / contract the Responsible Party shall prepare a final statement of account, and send it to the relevant Parties for payment. After receiving proof of payment for work performed, the Responsible Party shall release the file and contents/records contained therein, to the relevant Parties.

9.2 The Parties indemnify the Responsible Party from any loss of Personal Information, provided reasonable steps were taken to prevent such a loss.

10. SAFEGUARD

10.1 All documents and applications are located on a Windows Server and access are controlled by Active Directory Access Controlled Lists/Groups. All computers and devices are password/PIN protected.

10.2 Emails are hosted in Microsoft's Office 365 cloud infrastructure and protected and secured by their build-in security systems. This includes malware scanning, phishing/spoofing prevention etc.

10.3 Internet traffic are scanned for viruses by an onsite Sophos firewall which includes IPS (Intrusion Prevention System) The firewall firmware always gets updated to the latest version, as soon as it gets released.

10.4 Remote working happens via their onsite Sophos firewall using an encrypted SSL Sophos VPN connection using a username and password as well as a digital certificate for authentication. Only specific users have VPN access.

10.5 ESET Endpoint antivirus are installed on all computers and servers to protect against viruses, ransomware and dangerous websites. Antivirus definitions updates happens every hour and program upgrades are installed as soon as it is released. Computers are continuously checked to verify that the antivirus is up to date.

10.6 Desktop and server operating systems are set to automatically install Windows security updates. Computers are constantly checked to verify that they are fully patched.

10.7 For disaster recovery, a full server backup is done daily to alternating external hard drives and taken off-site. The drives are kept securely in a safe at PF Technologies's premises. Regular restores are done to verify the state of the backups.